UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF TENNESSEE
AT GREENEVILLE

IN THE MATTER OF THE SEARCH OF THE REAL PROPERTY ON WHICH LIES A RESIDENCE LOCATED AT 361 TOM TREECE ROAD, MORRISTOWN, TENNESSEE 37814, INCLUDING ALL OUTBUILDINGS AND STORAGE AREAS WITHIN THE CURTILAGE ASSOCIATED WITH THE PROPERTY (a photograph of the area in which the residence is located is attached hereto and fully incorporated herein.)	2:19-MJ-141 JUDGE CORKER

AFFIDAVIT FOR SEARCH WARRANT

I, Travis Carrier, being duly sworn, do hereby depose and state the following:

1. I am a Special Agent with the U.S. Department of Homeland Security ("DHS"), Homeland Security Investigations ("HSI"), Immigration and Customs Enforcement ("ICE"), assigned to the office of the Resident Agent in Charge, Knoxville, Tennessee, and have been employed by HSI/ICE for 11 years.

2. I am responsible for investigating offenses involving interstate travel with intent to engage in illegal sexual acts with children, as well as the possession, distribution, receipt, transportation, production, advertising, and accessing with intent to view of child pornography. My responsibilities include enforcing federal criminal statutes involving the sexual exploitation of children, including, but not limited to 18 U.S.C. §§ 2252, and 2252A.

3. I have received training and have experience relating to Federal Criminal Procedures, federal statutes, and U.S. Customs Regulations. I have also received training and instruction in the investigation of child sexual exploitation, including child pornography offenses. I have conducted, coordinated, and/or participated in numerous investigations relating to the sexual exploitation of children. I have participated in numerous search warrant executions by HSI, as

well as state and local police departments, and have participated in numerous seizures of computer systems and other evidence involving child exploitation and/or child pornography offenses. I have applied for and executed numerous search warrants pertaining to the sexual exploitation of children.

4. I, SA Travis Carrier, make this affidavit in support of an application for a warrant to search the property located at 361 Tom Treece Rd, Morristown, TN 37814. (herein referred to as the "Subject Premises"), described further in Attachment A, for evidence, instrumentalities, fruits, and contraband described further in Attachment B, concerning enticement violations, and the possession and distribution of child pornography, in violation of 18 U.S.C. §§ 2252, and 2252A.

5. The statements in this affidavit are based on my personal observations, my training and experience, my investigation of this matter, and information obtained from other law enforcement agents. Because this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth the facts that I believe necessary to establish probable cause to believe that evidence of a crime, contraband, fruits of crime, or other items illegally possessed, or property designed for use, intended for use, or used in committing crimes, in violation of 18 U.S.C. §§ 2252, and 2252A are located at , described further in Attachment A.

DEFINITIONS

6. The following definitions apply to this Affidavit and to Attachment B:

a. "Child erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit conduct.

b. "Child pornography," as used herein, includes the definition in 18 U.S.C. § 2256(8), which defines child pornography as any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct; (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct; or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct, as well as any visual depiction, the production of which involves the use of a minor engaged in sexually explicit conduct. 18 U.S.C. §§ 2252 and 2256(2).

c. "Visual depictions" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. 18 U.S.C. § 2256(5).

d. "Sexually explicit conduct" means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any persons. 18 U.S.C. § 2256(2).

7. "Computer" as used herein, is an electronic, magnetic, optical, electrochemical, or other high-speed data processing device performing logical or storage functions and includes a data storage facility or communications facility directly related to or operating in conjunction with such device. Such a device includes cellular smartphone telephones which allows users to place phone calls, has a digital camera, internet browsing capabilities, the ability to run software applications, as well as the ability to store data on the phone.

8. "Computer hardware" as used herein, consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

9. "Computer software" as used herein, is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

10. "Computer-related documentation" as used herein, consists of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, computer software, or other related items.

11. "Computer passwords and data security devices" as used herein, consists of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched.

Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

12. "Internet Protocol address" or "IP address" refers to a unique number used by a computer to access the Internet. IP addresses can be dynamic, meaning that the Internet Service Provider (ISP) assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet.

13. The terms "records," "documents," and "materials," as used herein, include all information recorded in any form and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings; cassettes; compact discs; electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks; as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

14. Internet cloud storage, file hosting service, cloud storage service, online file storage provider, or cyber locker are Internet hosting services specifically designed to host user files. It allows users to upload files that could then be accessed over the Internet from multiple computers, tablets, smart phones or other networked devices, by the same user and by other users, after a password or other authentication is provided. Related services are content-displaying hosting

services (i.e., video, image and music), virtual storage, and remote backup. Personal file storage services are aimed at private individuals, offering a sort of "network storage" for personal backup, file access, or file distribution. Users can upload their files and share them publicly or keep them password-protected. Some of the major providers of these services are known as Dropbox, SkyDrive, iCloud, Amazon Cloud Drive and Google Drive.

SUMMARY OF INVESTIGATION

15. On or about, 03/02/2019, Hamblen County Sheriff's Office (HCSO), responded to the "Subject Premises" in reference to images of child pornography discovered on a computer belonging to Robert Scott BROOKS. The complainant, Lori Turner, owner of the "Subject Premises", Robert Scott BROOKS's aunt, and caretaker for Robert Scotts BROOKS called 911 to report the discovered child pornographic images. Robert Scott BROOKS, who suffers from paraparesis, and resides at the "Subject Premises" asked Alysa Turner, daughter of Lori Turner and an additional caretaker for Robert Scott Brooks to format an SD-Card for him. Alysa Turner agreed to assist. Upon obtaining Robert Scott BROOKS's computer, she and Caleb Ferrell, a friend of Alysa Turner , also a caretaker for Robert Scott Brooks, observed what appeared to them as images of nude prepubescent girls on Robert Scott BROOKS's computer screen. Alysa Turner and Caleb Ferrell also reported seeing images labeled as 11- year old girls nude. Alysia Turner and Caleb Ferrell reported seeing images (thumbnails) of what appeared to be hundreds of nude prepubescent girls on the same computer (computer's screen) belonging to Robert Scott BROOKS. Alysia Turner and Caleb Ferrell showed the described images to Lori Turner. Lori Turner called 911 and reported the incident. HCSO Deputy Donnie Davis responded to this incident and made the initial report. Lori Turner later advised HCSO, Robert Scott BROOKS stated, regarding the described images, that he couldn't help himself and he had been addicted to porn for many years.

16. In response to the discovery of the child pornography, HCSO seized the following items from Robert Scott Brooks.

SEIZED ITEMS

- Red Amazon tablet: SL056ZE
- Black Amazon tablet: RSR87CV
- Black Amazon tablet: SLO56ZE
- Black TCL smart-phone
- White LG smart-phone

17. On 03/16/2019, HCSO obtained a search warrant for the above described electronic devices belonging to Robert Scott BROOKS.

18. On 04/18/2019, HCSO turned over the described seized items to Homeland Security Computer Forensic Agent (CFA) Brian Wall. HCSO requested HSI provide assistance conducting a forensic search of the above described seized items. CFA Wall began his examination on 04/18/2019.

19. On 05/02/2019, CFA Wall provided SA Carrier with a description of (6) videos containing child pornography discovered during the (ongoing) examination of the described seized items belonging to Robert Scott Brooks. The videos are described below.

DESCRIPTION OF VIDEOS

Video 1: File name vid_20171113_011133.mp4, depicts an adult male and an infant male toddler. The adult male is seen anally penetrating the toddler from behind. The toddler in the video is seen with what appears to be a blue binky in his mouth. This video is 2 mins and 46 Sec.

Video 2: File name quartet.avi, depicts 3-4 pubescent girls flashing their butts and vaginas in front of the camera. The video shows the girls' vaginas and at one-point anal penetration with

what appeared to be a dildo. Each girl is displayed in front of the camera and begins to fondle themselves while spreading open their vaginas. This video is 12 mins and 3 secs.

Video 3: File name amber2.wmv depicts a prepubescent female and an adult male. The beginning of the video depicts the female performing oral sex on the adult male's penis. Then the female strips down while lying on a bed in a manner that exposes her genitalia. The female then precedes to penetrate herself with what appears to be a clear dildo. This video is 5 mins and 40 secs.

Video 4: File name JM01.mp4, depicts a prepubescent female and an adult male. The female is nude and laying on her back. The adult male is seen with his penis out over top of the girl as the girl begins to masturbate the male individual. The adult male proceeds to ejaculate on the girl. This video is 1 min and 11 secs.

Video 5: File name video_2018-11-15_14-04-25.mp4, depicts a prepubescent female that looks to be Hispanic and an adult male. The video begins with the female performing oral sex on the adult male. The adult male begins to vaginally penetrate the female before ejaculating on the outside of her vagina. This video is 1 min and 20 secs.

Video 6: File name 1414813402876.mp4, depicts a prepubescent female laying on her back with an adult male penetrating her vaginally. The male individual also ejaculates in and on to the female's genitals. This video last 28 secs.

BACKGROUND INFORMATION CONCERNING CHILD PORNOGRAPHY

20. Based upon my own knowledge, training, and experience in child exploitation and child pornography investigations, and the experience and training of other law enforcement officers with whom I have had discussions, computers affect the methods used by people who possess, receive, distribute, and transport child pornography in these ways:

a. those who create child pornography can produce both still and moving images directly from a common video or digital camera, and other devices that create video and still images, including most cellular telephones and PDAs (e.g., a Blackberry). Images from such devices can be transferred to a computer by attaching the device to the computer using a cable, or by uploading images from the device's memory card directly onto the computer. Once on the computer, images can then be stored, manipulated, transferred, or printed. This includes transfer to some of the same types of devices that are commonly used to create child pornography, such as cellular telephones and PDAs, as well as computers. As a result of this technology, it is relatively inexpensive and technically easy to produce, store, and distribute child pornography. Cellular telephones are routinely backed-up to computers as not to lose any data that is stored on a cellular telephone if that cellular telephone is lost or damaged. I know this to have occurred with a Knoxville Police Department Internet Crimes Against Children investigation in which much of the evidence recovered was located on the suspect's computer as a result of the violator backing up his cell phone.

b. the Internet allows any computer to connect to another computer. Electronic contact can be made to literally millions of computers around the world. The Internet allows users, while still maintaining anonymity, to locate (i) other individuals with similar interests in child pornography; and (ii) websites that offer images of child pornography. Child-pornography collectors can use standard Internet connections, such as those provided by businesses, universities, and government agencies, to communicate with each other and to distribute child pornography. They can also distribute and collect child-pornography materials with peer-to-peer ("P2P") file sharing, which uses software to link

computers together through the Internet to form a network that allows for the sharing of digital files among users on the network. These communication links allow contacts around the world as easily as calling next door. Additionally, these communications can be quick, relatively secure, and as anonymous as desired. All of these advantages, which promote anonymity for both the distributor and recipient, are well known and are the foundation of transactions between child-pornography collectors over the Internet.

c. the computer's capability to store images in digital form makes it a common repository for child pornography. Internal and external computer hard drives typically store vast amounts of data, and hard drives with the capacity of 500 or more gigabytes – which can store tens of thousands of images at very high resolution – are not uncommon. Other electronic storage media, such as thumb drives and memory sticks, can store hundreds of images and dozens of videos. Likewise, optical storage media, which includes CD-ROMs and DVDs, and electromagnetic storage media, such as floppy disks, also can hold hundreds of images and multiple videos. Such electronic, optical, and electromagnetic storage media are very commonly used by those who collect child pornography to store images and videos depicting children engaged in sexually explicit activity. Agents who execute child-pornography search warrants often find electronic, optical, and/or electromagnetic storage media containing child pornography in the same location as or near the computer that was used to obtain, access, and/or store child pornography.

21. My training and experience, and the training and experience of other agents whom I have consulted, have shown the following:

a. Individuals who possess, transport, receive, and/or distribute child pornography often collect sexually explicit materials, which may consist of photographs;

magazines; motion pictures; video tapes; books; slides; computer graphics or other images; as well as literature describing sexually explicit activity involving children. Such individuals frequently store their child pornography on multiple electronic, optical, and/or electromagnetic storage media, including not only their computer, but also on external hard drives; floppy disks; CD-ROMs; DVDs; memory sticks; thumb drives; cell phones; PDAs; and other such media. Many of these individuals also collect child erotica, which consists of items that may not rise to the level of child pornography, but which nonetheless serves a sexual purpose involving children.

b. Individuals who possess, transport, receive, and/or distribute child pornography often seek out like-minded individuals, either in person or on the Internet, to share information and trade depictions of child pornography and child erotica. The different Internet-based vehicles used by such individuals to communicate with each other include, but are not limited to, P2P; e-mail; e-mail groups; bulletin boards; Internet Relay Chat; newsgroups; instant messaging; and other similar interfaces.

c. Individuals who possess, transport, receive, and/or distribute child pornography often collect; read; copy; or maintain names, addresses (including e-mail addresses), phone numbers, or lists of persons who have advertised or otherwise made known in publications and on the Internet, that they have similar sexual interests. These contacts are maintained as a means of personal referral, exchange, or commercial profit. These names may be maintained in the original

medium from which they were derived, in address books or notebooks, on computer storage devices, or merely on scraps of paper.

d. The majority of individuals who possess, transport, receive, and/or rarely dispose of their sexually explicit materials and commonly retain their collection of child pornography for long periods of time, even for years, in order to retain and gain easy access to child pornography that they have collected, sometimes with considerable effort. These individuals may go to great lengths to conceal and protect from discovery, theft, and damage their collections of illicit materials. These individuals almost always maintain their collections in the privacy and security of their homes or other secure location. These individuals may keep their collections in locked containers including filing cabinets, safes, or lockboxes. These individuals may also maintain their collections in password-protected or encrypted electronic media. They may keep these passwords, and other information concerning their use of the computer, on handwritten or printed notes that they store in personal areas and around the computer.

e. Possessors, traders, and distributors of child pornography sometimes store their illegal images and videos online in remote storage accounts. Therefore, any records, documents, invoices and materials in any format or medium that concern online storage or other remote computer storage could indicate that a person at the Subject Premises is storing illegal material in an online storage account.

f. Files, logs, and records relating to P2P files can contain the names of files sent through the P2P service, as well as the date and time the files were transferred. These records could help identify the individual who transferred the child

pornography images at the Subject Premises. Additionally, these records can provide historical information about the trading of child pornography by individuals at the Subject Premises.

CHARACTERISTICS OF TRADERS AND COLLECTORS OF CHILD PORNOGRAPHY

22. Based upon my experience and training in child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals involved in the online trading and collection of child pornography (hereafter "collectors").

23. Collectors may receive sexual stimulation and satisfaction from contact with children, from having fantasies of children engaged in sexual activity or suggestive poses, or from literature describing such activity.

24. Collectors often have companion collections of child erotica. Child erotica are materials or items that are sexually suggestive and arousing to pedophiles, but which are not in and of themselves obscene or pornographic. Such items may include photographs of clothed or partially-clothed children, drawings, sketches, fantasy writings, pedophilic literature and sexual aids.

25. Collectors also may correspond with and/or meet others to share information and materials. They may save correspondence from other child pornography collectors, including contact information like e-mail addresses, written, descriptions of others' sexual encounters with or molestation of minors, diaries, and saved online chats. The collectors typically conceal such correspondence as they do their sexually explicit material.

26. The storage of such materials in password-protected e-mail accounts and online remote data storage, to which only the collector has access, is a convenient way for collectors to trade, retain and amass child pornography while keeping the child pornography and conversations with other collectors hidden from others, such as family members, who share or may have access to the computer.

27. Collectors are known to retain child pornography for long periods of time, even for years, in order to retain and gain easy access to child pornography that they have collected, sometimes with considerable effort.

SPECIFICS REGARDING SEARCHES OF COMPUTER SYSTEMS

28. Based upon my training and experience, and the training and experience of specially trained computer personnel whom I have consulted, searches of evidence from computers commonly require agents to download or copy information from the computers and their components or remove most or all computer items (computer hardware, computer software, and computer-related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following:

a. Computer storage devices can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it with deceptive file names. This requires searching authorities to examine all the stored data to determine whether it is included in the warrant. This sorting process can take days or weeks, depending on the volume of data stored, and it would be generally impossible to accomplish this kind of data search on site.

b. Searching computer systems for criminal evidence is a highly technical process, requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure which is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

29. In order to fully retrieve data from a computer system, the analyst needs all storage media as well as the computer. In cases involving child pornography where the evidence consists partly of graphics files, the monitor(s) may be essential for a thorough and efficient search due to software and hardware configuration issues. The analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard disk or on external media).

30. In addition, a computer, its storage devices, peripherals, and Internet connection interface may be instrumentalities of the crime(s), within the meaning of 18 U.S.C. §§ 2251 through 2256 and are subject to seizure as such if they contain contraband or were used to obtain or store images of child pornography.

PROCEDURES TO BE FOLLOWED IN SEARCHING COMPUTERS AND COMPUTER STORAGE MEDIA

31. With respect to the search of any computers or electronic storage devices seized from the location identified in Attachment A hereto, the search procedure of electronic data contained in any such computer may include the following techniques (the following is a non-exclusive list, and the government may use other procedures that, like those listed below, minimize the review of information not within the list of items to be seized as set forth herein):

a. examination of all of the data contained in such computer hardware, computer software, and/or memory storage devices to determine whether that data falls within the items to be seized as set forth herein;

b. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) instrumentality of the offenses; (2) a fruit of the criminal activity; (3) contraband; (4) otherwise unlawfully possessed; or (5) evidence of the offenses specified above);

c. surveying various file directories and the individual files they contain to determine whether they include data falling within the list of items to be seized as set forth herein;

d. opening or reading portions of files in order to determine whether their contents fall within the items to be seized as set forth herein;

e. scanning storage areas to discover data falling within the list of items to be seized as set forth herein, to possibly recover any such recently deleted data, and to

search for and recover deliberately hidden files falling within the list of items to be seized; and/or

f. performing key word searches through all storage media to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment B.

CONCLUSION

32. Based on the above information, I respectfully submit that there is probable cause to believe that violations of possession and receipt of child pornography offenses, in violation of 18 U.S.C. §§ 2252 and 2252A, have been committed, and that evidence, instrumentalities, fruits, and contraband relating to this criminal conduct, as further described in Attachment B, will be found in the "Subject Premises", as further described in Attachment A.

33. I therefore respectfully request that this Court issue a search warrant for the property located at 361 Tom Treece Rd. Morristown, TN 37814, and is described as a tan/yellow, single-story, ranch style residence, more particularly described in Attachment A, authorizing the seizure of the items described in Attachment B.

FURTHER AFFIANT SAYETH NOT.

Travis Carrier
Special Agent
Homeland Security Investigations

Subscribed and sworn to before me
this 6th day of May, 2019.

CLIFTON L. CORKER
United States Magistrate Judge

ATTACHMENT A

DESCRIPTION OF PREMISES TO BE SEARCHED

The subject premises, including out- buildings, and outbuildings within/on the said curtilage of 361 Tom Treece Rd, Morristown, TN 37814, located in Hamblen County. The property is described as a yellow/tan ranch style, single-story residence located on 361 Tom Treece Rd, Morristown, TN 37814. There is a back deck and covered front porch. The residence appears to have brown doors and windows.

ATTACHMENT B

LIST OF ITEMS TO BE SEIZED AND SEARCHED

1. Any cellular telephone, personal digital assistant, computer(s), computer hardware, computer software, removable digital media, computer related documentation, computer passwords and data security devices, videotapes, video recording devices, video recording players, and video display monitors that may be, or are used to: visually depict child pornography or child erotica; display or access information pertaining to a sexual interest in child pornography; display or access information pertaining to sexual activity with children; or distribute, possess, or receive child pornography, child erotica, or information pertaining to an interest in child pornography or child erotica.

2. Any and all computer software, including programs to run operating systems, applications (such as word processing, graphics, or spreadsheet programs), utilities, compilers, interpreters, and communications programs.

3. Any and all notes, documents, records, or correspondence, in any format and medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and handwritten notes) pertaining to the possession, receipt, or distribution of child pornography as defined in 18 U.S.C. § 2256(8) or to the possession, receipt, or distribution of visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2).

4. In any format and medium, all originals, computer files, copies, and negatives of child pornography as defined in 18 U.S.C. § 2256(8), visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2), or child erotica.

5. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and handwritten notes), identifying persons transmitting, through interstate or foreign commerce by any means, including, but not limited to, by the United States Mail or by computer, any child pornography as defined in 18 U.S.C. § 2256(8) or any visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).

6. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) concerning communications between individuals about child pornography or the existence of sites on the Internet that contain child pornography or that cater to those with an interest in child pornography.

7. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) concerning membership in online groups, clubs, or services that provide or make accessible child pornography to members.

8. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) that concern any accounts with an Internet Service Provider.

9. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) that concern online storage or other remote computer storage, including, but not limited to, software used to access such online storage or remote computer storage, user logs or archived data that show connection to such online storage or remote

computer storage, and user logins and passwords for such online storage or remote computer storage.

10. Any and all address books, mailing lists, supplier lists, mailing address labels, and any and all documents and records, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files), pertaining to the preparation, purchase, and acquisition of names or lists of names to be used in connection with the purchase, sale, trade, or transmission, through interstate or foreign commerce by any means, including by the United States Mail or by computer, any child pornography as defined in 18 U.S.C. § 2256(8) or any visual depiction of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).

11. Any and all documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files), pertaining to occupancy or ownership of the premises described above, including, but not limited to, rental or lease agreements, mortgage documents, rental or lease payments, utility and telephone bills, mail envelopes, or addressed correspondence.

12. Any and all notebooks, notes, and any other records reflecting personal contact and any other activities with minors visually depicted while engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).